Vendor Risk Assessments

Software Assurance Forum
Department of Homeland Security

MITRE, McLean, Virginia

March 11, 2009

Agenda

- **Introductions**
- **Shared Assessments Program**
  - Background
  - Roadmap
- **Vendor Risk is Business Risk**
- **Financial Institution (FI) & Service Provider (SP)**
  - Standardization and Efficiency
  - Maximize brand & information protection
  - Program effectiveness and benefit realization

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Charles Miller, The Santa Fe Group
Senior Consultant

The Santa Fe Group www.santa-fe-group.com

- A strategic consulting company providing unparalleled expertise to leading financial institutions and other critical infrastructure companies.
- **The Shared Assessments Program,**
  - Introduced in partnership with BITS to evaluate service provider security practices, raise awareness on controls and boost the efficiency of the vendor assessment process.
- **The Vendor Council**
  - Forum for vendors to engage in dialogue with the financial industry on key issues. Committed to innovative and collaborative solutions that address common and emerging challenges.

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

M. Eric Johnson, Tuck School of Business at Dartmouth College - Professor

- **Center for Digital Strategies**
  - Brings together executives, academics, and students to examine the role of digital strategies in creating competitive advantage.
  - Focuses on enterprise CIOs.
  - Runs the CIO Roundtable.
    - http://mba.tuck.dartmouth.edu/digital/About_the_Center/TLRDS.html

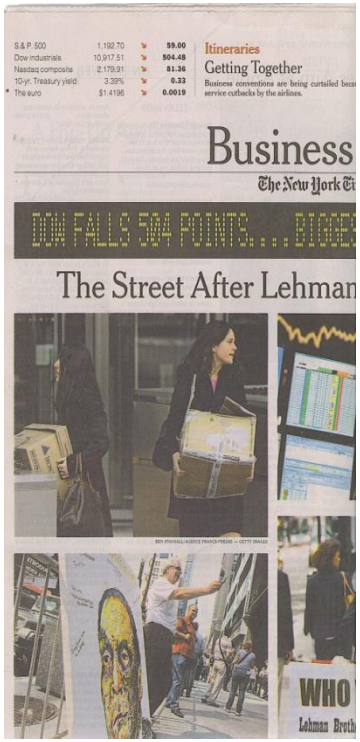
- **Related Research**
  - Extended enterprise risk management.
    - Evaluating and communicating risk.
    - http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/ResearchSecurity.html
  - Vendor information risk rating.
    - Market mechanisms for adoption

Ken Peterson, Churchill & Harriman
President & CEO

- **Churchill & Harriman**
  - Performed 700+ Global Risk Assessments since 1998
  - Several clients with Infrastructure designated as Critical by DHS
  - Risk mitigation clients include the Federal Reserve Bank, DTCC, PhRMA
  - Certain results contributed to viewed as Best Practices at the highest level of the U.S. Federal Government
  - First approved IS0 27001 and BS 25999 Associate Consultancy by The British Standards Institute
  - Consult to global organizations on Vendor Management Program elements
- **Assessment Services**

info@chus.com

Economic Crisis – Outsourcing Impact



- **Restructuring**
  - Financial industry: closings, mergers, acquisitions …
  - Outsourcers: closures, consolidations, mergers, new countries …
- **Pressure**
  - Cost, FTE reductions, knowledge drain
  - Outsourcers – same or more for less
- **Risk**
  - Reputational – data breach and data leakage
  - Fraud – internal, external, vendors (supply chain weak link)
  - Countries with different maturity levels for legal / privacy laws / frameworks

The revelation of fraud has prompted many of Satyam's 53,000 employees to look for new jobs. Noah Seelam / AFP

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Shared Assessments Program

- **Created by BITS Members**
  - Industry recognition of the need to protect our clients and our business models
  - IT Service Providers Expectations Matrix
- **Formation of the Program**
  - Proof of concept
  - Operational recommendations
- **Objectives**
  - Raise the bar on risk management and controls
  - Reduce costs and increase efficiency
  - Provide a forum for industry collaboration
  - Develop a common-sense approach and evolve to remain relevant
- **Program is member funded with artifacts available to all**

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Assessment Tools

- **Standardized Information Gathering (SIG) Questionnaire**
  - Replaces proprietary institution questionnaires
  - Complete picture of provider operations and controls
  - Questions are risk tiered and once completed by service providers, can be distributed to all clients
  - Documented relationship to industry standards (ISO, COBIT and PCI)
  - Addition of XML support for completion of the SIG
- **Agreed Upon Procedures (AUP)**
  - Objectively test a control and report results
  - Test and validate service provider information security controls
  - Institutions view results in the context of their risk management requirements

Controls*

- Risk Management
- Information Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

* ISO 27002 Information Security Management Control Areas

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

The SIG Questionnaire & Structure

- Replaces proprietary outsourcer questionnaires with a collaborative industry standard
- Ideally completed a single time by each vendor
- Constructed a series of high-level questions
- Sufficient to address risk management and compliance needs associated with relatively less risky outsourced functions
- SIG Version 4.0 Enhancements:
  - Completed comprehensive, documented review and alignment with the AUP and ISO 27002:2005 standards and industry standards (ISO, COBIT and PCI)
  - Established three risk levels within a comprehensive SIG tool
  - Automated SIG Management Tool to compare past versions of the SIG
  - Addition of XML support for completion of the SIG

Agreed Upon Procedures

- Developed collaboratively to comply with AICPA standards
- Test hardware, software and processes within vendor's designated target systems
- In conjunction with an on-site assessment, objectively tests, validates and reports back on examined controls
- Outsourcers view results in the context of their risk management requirements
- **AUP Version 4.0 Enhancements:**
  - Documented relationship to industry standards (ISO 2700, COBIT, PCI)
  - Added a program guide aligned by business type
  - Added individual business objective for each AUP
  - Added 7 new AUPs and modified 11 existing AUPs

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Regulatory Focus

- Designate, in writing an employee(s) to coordinate the vendor governance program. (SEC)
- Qualified and knowledge personnel must manage the relationship.(FDIC)
- Maintain effective oversight and control throughout the relationship, assess risk through ongoing monitoring of controls. (OTS)
- Have a comprehensive vendor assessment risk management process to govern vendor relationships. Process should include: risk assessment, due diligence during selection, contract review and monitoring of service providers, periodically rank vendors according to risk and to determine level of monitoring required.(FFIEC)

Adoption Survey

- 131+ are completing SIG/AUP, including FIs as service providers
  - 81 available now
  - 50 more available in 2009
- 280+ willing to leverage SIG/AUP reports
  - 37 more plan to leverage in 2009
- 72 using SIG as default questionnaire with service providers
  - 42 more plan to use in 2009

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

2009 Roadmap

- Explore synergies with industry organizations (e.g., IAPP, SIFMA)
- Expand awareness and adoption to other sectors (e.g., higher education, healthcare, retail, telecom)
- Continue to promote adoption by US financial institutions and their service providers
- Expand education and outreach to strategic foreign countries through organizations such as NASSCOM
- Explore enhancements around privacy, GLBA, HIPAA, PCI 1.2, and other industry standards
- Public policy outreach
- Framework concept: productivity and consistency of audits and assessments

Privacy Initiative

- **Program Established**
  - Launched January 2009
  - Representation from the Shared Assessments Program membership, IAPP, Legal, Big 4 and BITS
- **Objectives**
  - Include privacy requirements as part of SIG and AUP assessment tools
  - Standard control questions and procedures for use by service providers in achieving and demonstrating compliance with state laws and regulations

Membership Today: Financial Institutions

- Bank of America Corp.
- The Bank of New York Mellon
- Bank of Tokyo Mitsubishi
- Citi
- Goldman Sachs
- JPMorgan Chase
- Merrill Lynch
- Morgan Stanley
- M&T Bank
- Target Corporation
- The Depository Trust & Clearing Corporation
- US Bancorp
- Wachovia Corp.
- Wells Fargo & Company
- Wilmington Trust Co.

- The **internal costs for vendor security** assessments has been **reduced to less than 10% of last year's cost** primarily through the use of the AUP as one our requirements for SPs that …access sensitive information

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Membership Today: Service Providers

- Acxiom
- Convergys
- Early Warning Services
- Equifax
- Experian
- First Data
- IBM
- Infosys Technologies Ltd.
- Iron Mountain
- LiveOps
- Radian Group Inc.
- SEI
- SunGard
- TSYS
- Usi, an AT&T Company
- VeriSign
- Wipro
- Yodlee
- Zoot Enterprises

- "Not only does the program **save our company time and resources…**our customers also benefit by getting the information they need immediately."
- "We have also been able to **reassign two FTE to other strategic initiatives** as a direct result of the program."

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Membership Today: Assessment Firms

- Accuvant
- AsTech Consulting
- BSI Management Systems America, Inc.
- CDI IT Solutions
- Churchill & Harriman
- Deloitte & Touche*
- Ernst & Young*
- FishNet Security
- KPMG*
- NET2S
- PricewaterhouseCoopers*
- Trustwave Holdings, Inc.
- VeriSign
- Verizon Business

**Technical Advisers*

- "The FIs like the fact that they are **basing an internal standard on an industry benchmark**. Our organization has been very successful working with organizations in getting questionnaires and establishing a risk management baseline **utilizing industry recognized processes and procedures."**

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Financial Institution

Vendor Management Program - Challenges

- Design and implement a vendor management program based on industry standard practices leveraging the Shared Assessments Program for service providers to DTCC
- Include key stakeholders: CEO, CISO, CPO, Legal, Procurement
- Interested in standardization and reducing the cost of vendor security assessments

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Program Implementation

Approach

- Prepared a SIG for DTCC as a service provider
- Hired Churchill & Harriman and completed the AUP
- Leveraged the adoption lessons of the BITS Shared Assessments Program to design and implement the vendor management program
- Created 3 tiers of service providers with specific security requirements for each
- Updated contract language to align with tiers
- 3rd tier service providers need to complete SIG (full), AUP in addition to other requirements (TLS, contract, employee background check, etc.)

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Program Implementation

Vendor Forum

- Seventy attendees participated in-person, ½-day vendor forum and many more took part by phone.
- The SIG and AUP each were explained in detail.
- Vendors benefited from each others' questions and comments regarding their own approaches to adopting the Shared Assessments Program.
- Follow-up information provided to each vendor
- Scheduled meetings with each tier 3 vendor to agree on adoption dates for the SIG and AUP.

Program Implementation

Benefits Realized

- **2007 / Pre Shared Assessments Implementation**
  - Total expenses for vendor management program security assessment requirements = **$300,000**
- **2008 / Post Shared Assessments Implementation**
  - Total expenses for vendor management program security assessment requirements = **$1,400**
- **Vendor Management Program enhancements**
  - Improved risk management capability
  - Substantially reduced costs

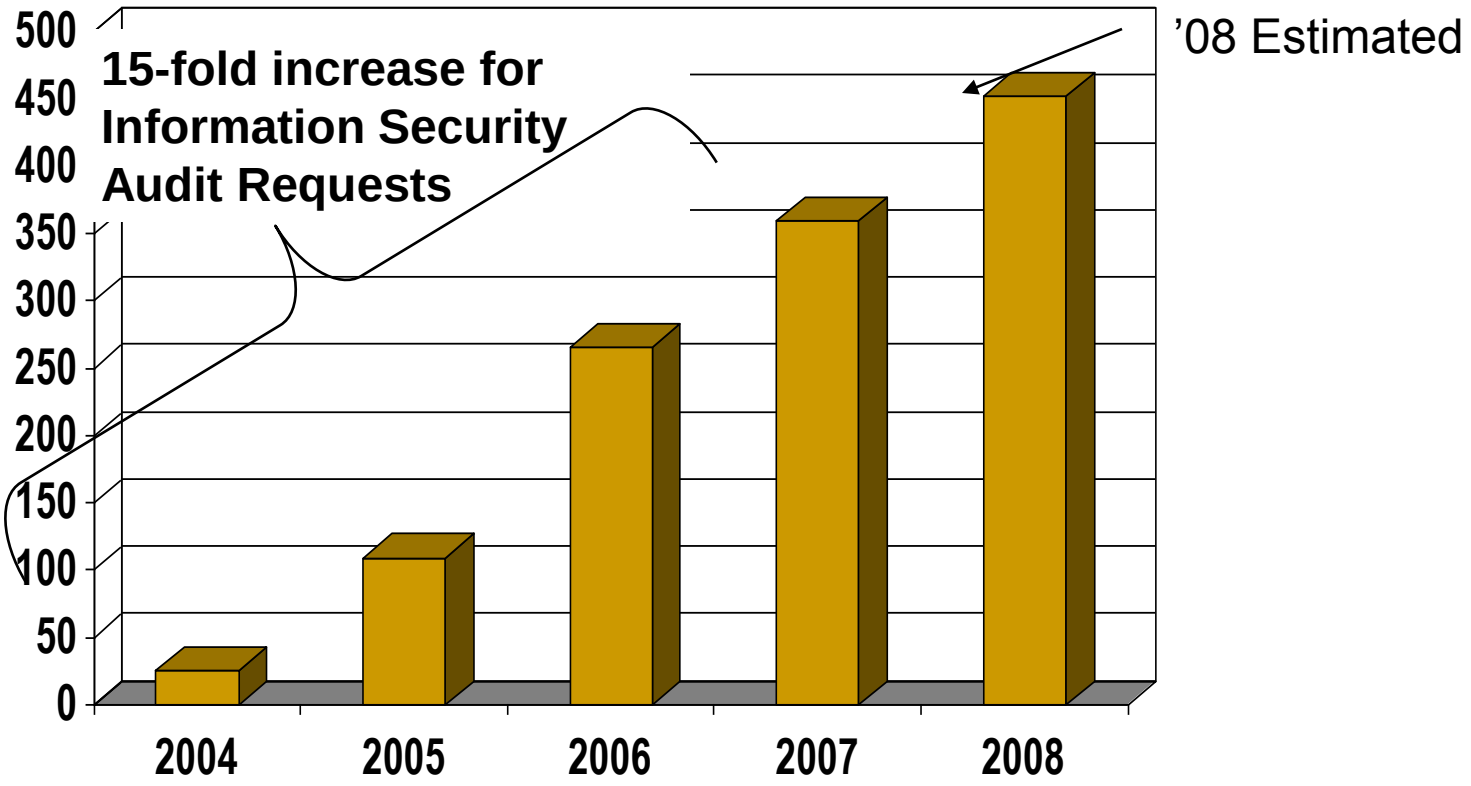
SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Service Provider

Vendor Management Program - Challenges

- Financial Industry is our largest vertical market
- Among the most heavily regulated in the world
- Often, large with multiple LOB's, departments and functions
- Customers continue Vendor Risk Management Program adoption
- Needed an Industry Standard!

Control Request Trends

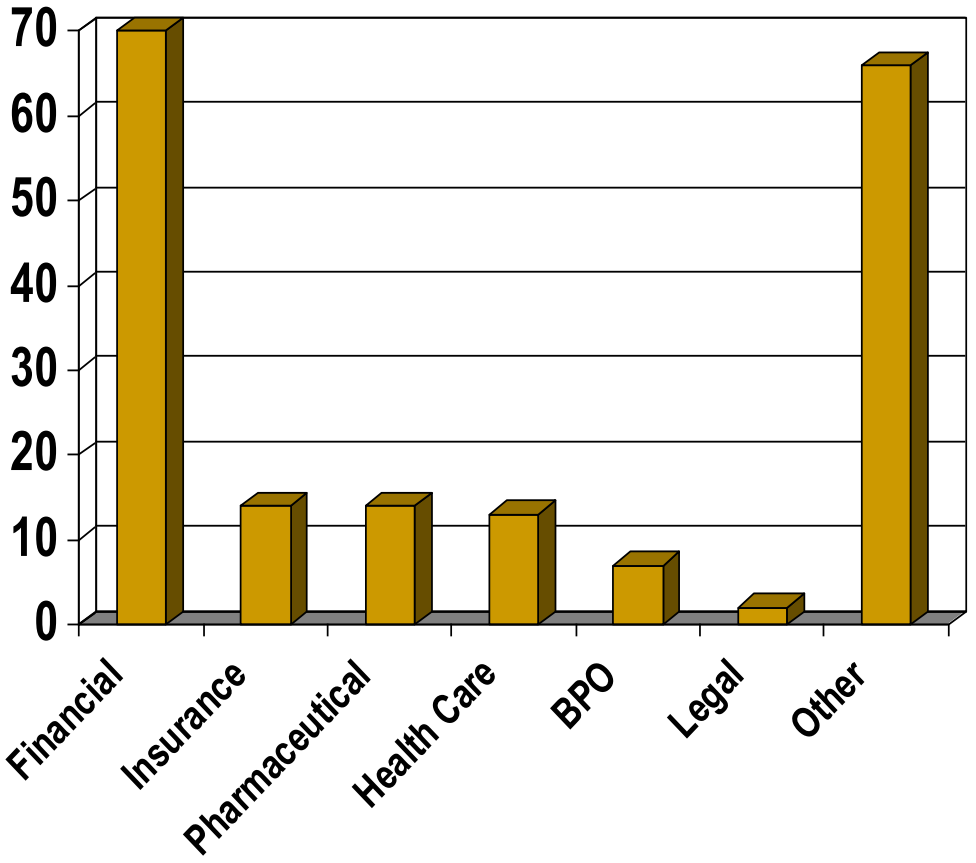


SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Program Implementation

Acceptance

- **SIG & AUP**
  - Distributed 181
    - Jan ’08 – Aug ’08
  - ~ 90% first time acceptance rate – no further remediation



SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE

Program Implementation

Benefits

- Saves time, money and human resources
- Customers benefit by getting the information they need immediately
- Reduces time to close deals on new third-party relationships
- Allows reassignment of limited key resources to other strategic initiatives
- Acceptance Rate

Closing thoughts

- Benefits are real and Savings can be significant!
- Outsourcing risks are increasing and will receive more focus and oversight going forward.
- Shared Assessments Program will provide an industry approved standardized vendor assessment approach

Questions

Thank you!

Contact Information

- Charlie Miller, Senior Consultant, The Santa Fe Group
  charlie@santa-fe-group.com
  718-705-1200
- Ken Peterson, President and CEO, Churchill and Harriman
  kpeterson@chus.com
  609-921-3551
- M. Eric Johnson, Professor, Tuck School of Business at Dartmouth
  m.eric.johnson@tuck.dartmouth.edu
  (603) 646-0526

For More Information

- Program information and resources:

  www.sharedassessments.org

- Upcoming events
  - Shared Assessments Summit

    Chicago, May 27-28

- Contacts:

Michele Edson
michele@santa-fe-group.com
831-637-1879

SHARED ASSESSMENTS | A PROGRAM OF BITS FINANCIAL SERVICES ROUNDTABLE